



QUALYS SECURITY CONFERENCE 2018

Out-of-band Configuration Assessment (OCA)

Make your Inaccessible, Sensitive Assets visible to your Vulnerability and Compliance Program

Shailesh Athalye

Director, Compliance Solutions

Qualys, Inc.

Agenda

Use-cases on why some of the big customers eagerly waiting

Workflow and the Demo

Content support

Roadmap

Use case:

Two of the biggest Banks

Disconnected/Inaccessible systems to be a part of overall Vulnerability, Risk and Compliance program

Sensitive Systems/Regulated Devices

Legacy Systems

Highly locked down systems

Network Appliances

Air-gapped Networks

» Adtran AOS
» BlueCoat ProxySG
» Brocade FabricOS
» Check Point GAIA
» Cisco IOS
» Dell Force10 FTOS
» Extreme ExtremeXOS
» FireEye
» Fortigate FortiOS
» HP ProCurve
» Huawei VRP
» Juniper Junos
» NetApp Data ONTAP
» SonicWALL SonicOS



Use case:

Visibility Matters to the...

search engine tech company and Healthcare network

**Impacts to security
program include:**



Incomplete Asset Inventory

Exposure to Unknown
Vulnerabilities &
Misconfigurations

Ineffective Risk Evaluation

Compliance in silos

Current Options

Ad-hoc scripts

Procedural controls
(manual assessment)

Outside audits

Limited software-based
solutions



Introducing Out-of-Band Configuration Assessment

OCA, add-on to VM/PC

Flexible Data Collection via
API/UI

Support for Inventory,
Policy Compliance and
Vulnerability Assessment

Bulk data, Automated and
Customizable

Qualys. Enterprise
Out-of-Band Config Assessment
g-frame-standard (123)

Assets

160 Assets

TECHNOLOGY

FireEye Appliance	78
Cisco UCS Server	13
IMB IMS	17
Brocade Switches	10
Acme Packet Net Platform	2
3 more	

SEVERITY

Severity 5	124
Severity 4	55
Severity 3	63
Severity 2	11
Severity 1	9

ASSET	OPERATING SYSTEM	NETBIOS	NETWORK	CREATED DATE
74.217.73.201 host1.example.com	FireEye CM:	COMPUTERNAME.1	N-name.here	Apr 11, 2018
74.217.73.201 host1.example.com	Cisco IOS 1	COMPUTERNAME.1	Network.Name	Apr 11, 2018
74.217.73.201 host1.example.com	WebSphere	COMPUTERNAME.1	Another-Network	Apr 11, 2018
192.168.255.255 host1.example.com	FireEye CMS 8.x	COMPUTERNAME.1	Network	Apr 11, 2018
74.217.73.201 host1.example.com	DCX-8510 7.1.0a	COMPUTERNAME.1	US-Headquarters	Apr 11, 2018
74.217.73.201 host1.example.com	FireEye CMS 8.x	COMPUTERNAME.1	Network-long-nam...	Apr 11, 2018
74.217.73.201 host1.example.com	WebSphere Liberty 9.0	COMPUTERNAME.1	PUNE	Apr 11, 2018

Configuration Upload Workflow

Push the Asset data

Upload Configuration Data

Qualys creates agent-based data snapshot

Report Generation

ASSET PROVISIONING

POST `http://{{base_url}}/oca/v1.0/asset`

GET `http://swarmm01.p17.eng.sjc01.qualys.com:53670/oca/v1.0/asset/03df1879-458c-495d-873d-7ab2daa34045/commands/PolicyCompliance`

```
1 {
2   "code": 200,
3   "data": {
4     "items": [
5       "version",
6       "tsclockserver",
7       "configshow -all",
8       "syslogdipshow"
9     ]
10  }
11 }
```

FORWARD COMMAND OUTPUTS FABRIC

POST `http://{{base_url}}/oca/v1.0/asset/03df1879-458c-495d-873d-7ab2daa34045/command/output/{{type}}`

Params Authorization Headers (3) Body Pre-request Script Tests

none form-data x-www-form-urlencoded raw binary

KEY	VALUE	DESCRIPTION
<input checked="" type="checkbox"/> configshow -all	<input type="button" value="Choose Files"/> No file chosen	
<input checked="" type="checkbox"/> syslogdipshow	syslog.1 10.170.65.31	
<input checked="" type="checkbox"/> tsclockserver...	Active NTP Server 10.170.158.12...	
<input checked="" type="checkbox"/> version	Kernel: 2.6.14.2 ...	
Key	Value	Description

Out-of-Band Configuration Assessment

Demo

OCA

GET swarmm01.p17.eng.sjc01.qualys.com:53670/oca/v1.0/technologies/PolicyCompliance

Params

KEY

VALUE

Key

Value

Pretty

Raw

Preview

JSON

```
1 [
2   "Data Domain OS 5",
3   "FireEye CMS 7",
4   "FireEye CMS 8",
5   "Imperva WebApplication Firewall",
6   "Fabric 7",
7   "Fabric 8",
8   "ACME Packet OS",
9   "Juniper IVE 8"
10 ]
```


Qualys OCA Benefits



Cover Your Blind Spots Quickly

For urgently required technologies, as an interim method till scanner or agent support is available



Flexible Data Collection

Fully automate data collection out-of-band via API or upload manually via the UI.



Complete Vulnerability & Compliance Visibility

Assess isolated, and locked-down systems for misconfiguration and vulnerabilities



Expanded Platform Coverage

Extends Qualys coverage to legacy and uncommon platforms, including network devices, applications, appliances, mainframes, and more.

Technology Support

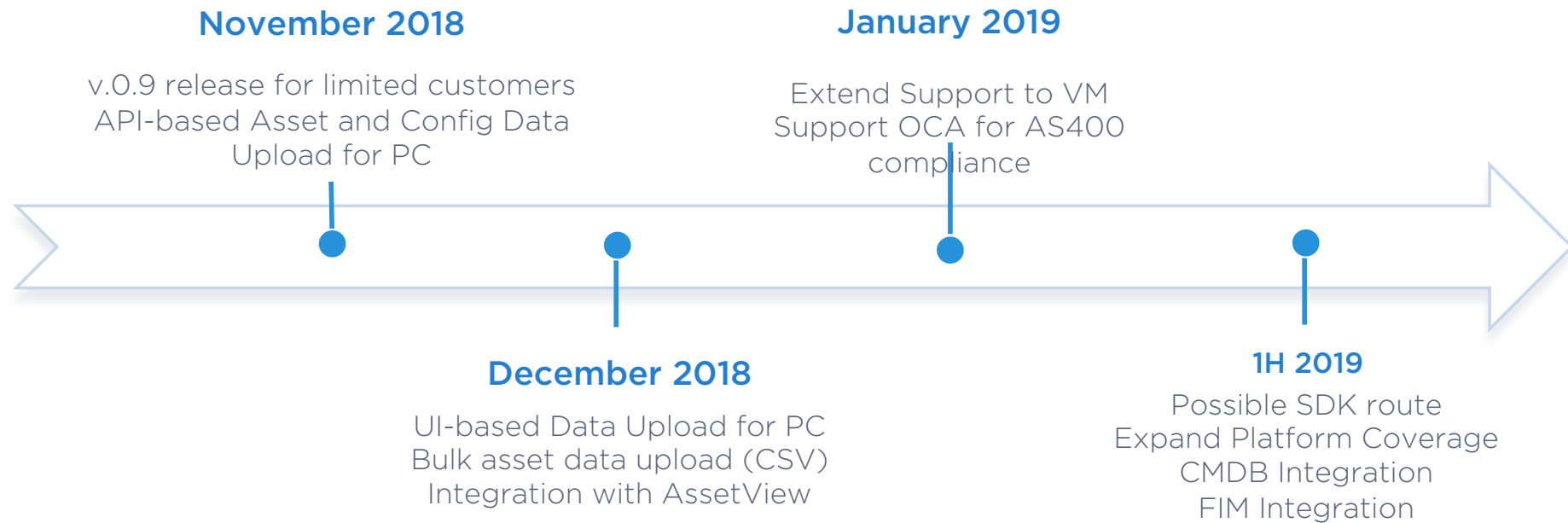
V0.9 and v1.0 release November - 2018

FireEye Appliances
BigIP F5
Brocade DCX Switch
Acme Packet Net
Imperva Firewall
Cisco Wireless Lan Controller 7
Cisco UCS Server
NetApp OnTap
Juniper IVE

Future Priorities

AS/400
Cisco Meraki
Sonic Firewall
Fortinet Firewalls
Aruba WLC
Dell EMC Data Domain
Oracle Tape Library

Availability & Roadmap





QUALYS SECURITY CONFERENCE 2018

Thank You

Shailesh Athalye
sathalye@qualys.com



QUALYS SECURITY CONFERENCE 2018

Security Assessment Questionnaire

Automate the Assessment of Procedural
Controls & Vendor Risk

Shailesh Athalye

Director, Compliance Solutions, Qualys, Inc.

Agenda

How SAQ compliments Qualys technical security Apps -
Internal Procedural controls Assessment
Vendor Control & Risk Assessment

Content support

Demo

Roadmap

Preview of Future use case: Customer risk management as a vendor

One of the biggest Financial Institute

Assesses their Internal Procedural and Process controls

Need to comply with number of International and regional mandates/ standards.



Took 2 hours to rebuild Excel based 76 question assessment using web-based UI and Out-of-box Rich content

They understand >50% compliance requirements are related to assessing processes and procedures



Dashboards the process deficiencies and risk posed by Internal controls failure

Important that Respondents find it easy and make the collected data actionable



Consolidates the Internal procedural control posture with Technical compliance controls







New-age Vendor Assessment Challenges

Extend the Perimeter to include vendors
- security & vulnerability data collection

Vendor Profiling based on the services,
Vendor Assessment based on criticality

Vendor control data aggregation with
Internal security and compliance data

Automated workflow, operational
dashboards

	SOURCE OF ATTACK	FINANCIAL IMPACT	REPUTATIONAL IMPACT	BREACH ORIGIN
	Attackers stole credentials from 3 rd Party vendor to breach network	\$200 million in costs (to date)	✓	<div>Direct Breach 30%</div> <div>Third Parties</div> <div>70%</div>
	Attackers breached network via 3 rd Party vendor	Estimated \$2-3 billion in fraud charges	✓	
	Breach due to 3 rd Party vendor	Estimated \$3 billion in fraud charges	✓	
	Google's Australia office hacked via 3 rd Party HVAC vendor	Impact TBD	✓	
	Yahoo Mail accounts hacked due to 3 rd Party database breach	Impact TBD	✓	
	T-Mobile customer PII data stolen from Experian (3 rd Party) server	15 million customers' PII stolen	✓	

One of the biggest pharma company

Assessing their vendor risk through SAQ



Vendors Profiling — Defines Criticality based on Service areas/Cybersecurity domains



Assesses vendors per their risk profile, in a standardized (SIG) manner



Uses out-of-the-box content, including regional mandates



Dashboards the risk posed by the highly critical vendors and ranks them per risk



Easy online workflow for the vendors, receives reminders, alerts and status



Consolidates the vendor control posture with Internal procedural & technical compliance controls

Rich Template Library

Industry

PCI DSS SAQ A, B, C, D
IT for SOX
GLBA
BASEL 3 (IT)
HIPAA
HITRUST
NERC CIP v5
SWIFT
NERC CIP

Popular Standards

ISO 27001-2013 ISMS
NIST CSF
COBIT 5
FedRAMP
COSO
ITIL
CIS TOP 20 Controls
**Shared Assessment
(SIG) *- vendor
assessment**

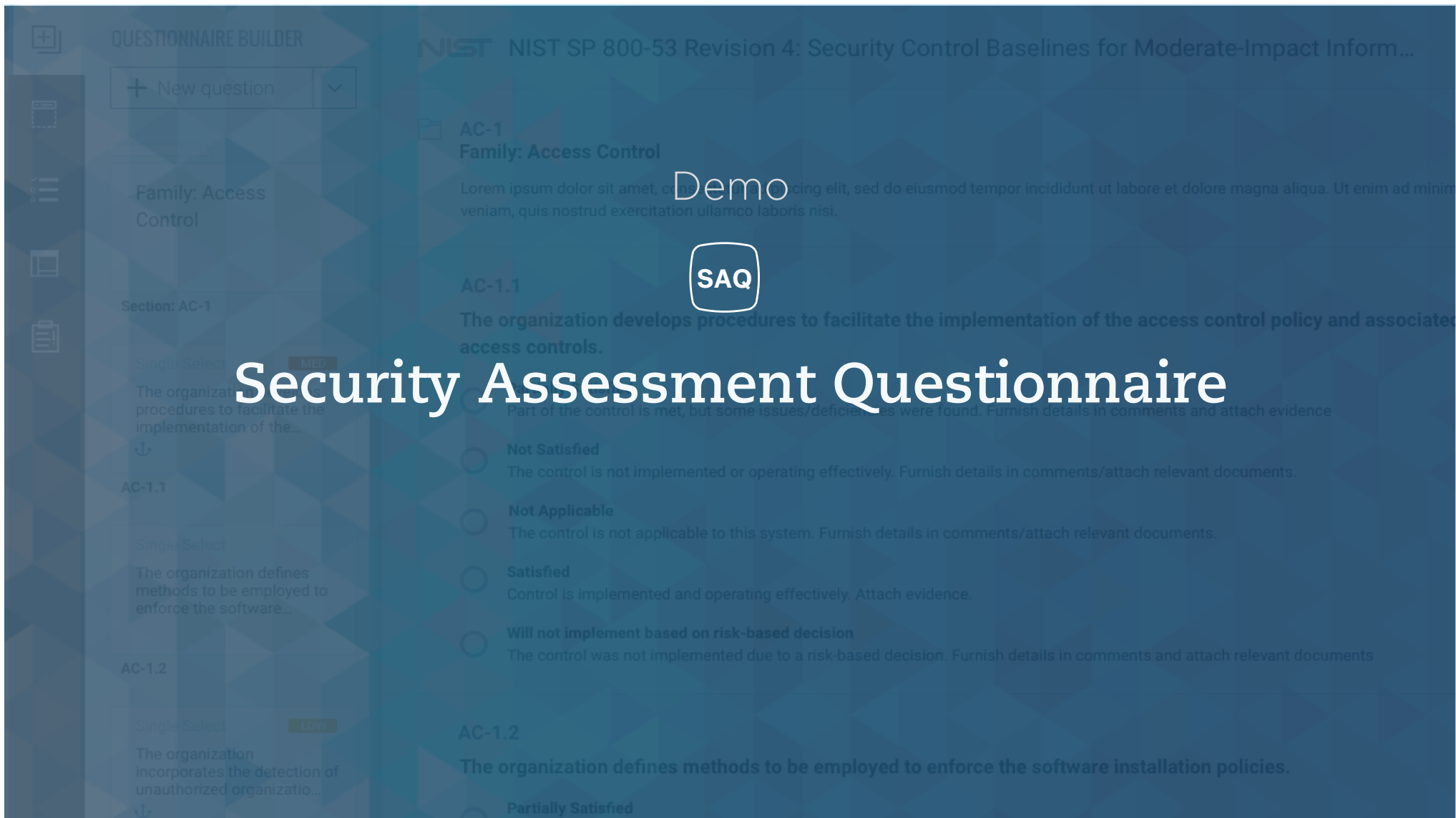
Regional

GDPR
Abu Dhabi Info Sec
Standards
ANSSI (France)
MAS IBTRM (Singapore)
BSP (Philippines)
BSI Germany
ISM (Australia)
UK Data Protection
RBI Guidelines (India)
California Privacy**
Canada Data Protection
2018**

Technical Services

CSA CAIQ v3.0.1
CSA CCM v3.0.1
Vendor Security for
Hosting Service Provider
AWS **
Procedural controls for
cloud, containers**

- ✦ Includes premium content – Shared Assessments (SIG)
- ✦ Use as-is or customize to your needs



SAQ Roadmap

Q3 2018

User/Role/Privilege Management
Question Bank
Create template from library templates
New campaign UI
Risk scoring

Q1 2019

Vendor-driven workflows to cater to customers

- Create answer bank,
- Upload customer required templates
- Match on Keywords
- Metrics, Dashboards on risk posed to my customers

Q4 2018

SAQ Lite – for PCI users
Vendor Risk Management workflows

- Vendor Onboarding, Profiling
- Automated assessment based on Vendor profiles/onboarding
- Compare vendors based on risk scores
- Dashboards on total Vendor risk/
Trending/Top 5 risky vendors

* Roadmap items are future looking; timing and specifications may change

In the world where everyone is a vendor of someone

SAQ Feature coming up in Q1: Answer bank

Technology company wants to understand Risk posed to the customers



Receives 100s of questionnaires from their customers and answers them offline, through spread-sheets



Want to understand What risk they pose to their critical customers



Costly & resource-intensive to respond and gains no visibility into risk intelligence



Want to understand the top failing, passing cybersecurity areas/ answers to improve their own internal controls



Wants to drive the vendor-management project to showcase their good security practices and use the data for contract negotiation





QUALYS SECURITY CONFERENCE 2018

Thank You

Shailesh Athalye
sathalye@qualys.com